REMARKS

Claims 28-52 are currently pending in the subject application, and are presently under consideration. Claims 28-52 are rejected. Favorable reconsideration of the application is requested in view of the comments herein.

In addition, Representative for Applicant is respectfully requesting withdrawal of the finality of the Office Action Rejection, in accordance with the discussion with supervisor Ayaz Sheikh on March 7, 2005. In the Office Action dated April 14, 2004, claims 1-8 and 11-27 were cancelled for the purpose of renumbering, due to the omission of claims 9 and 10 from the originally filed application, and were recast as claims 28-52. It is respectfully submitted that Representative for Applicant made no amendments to the claims upon renumbering them, such that claims 28-52 correspond directly to original claims 1-8 and 11-27. "Under present practice, second or any subsequent actions on the merits shall be final, except where the examiner introduces a new ground of rejection that is neither necessitated by applicant's amendment of the claims nor based on information submitted in an information disclosure statement..." (MPEP, §706.07(a)). Accordingly, because the Examiner introduced a new ground of rejection that was not necessitated by an amendment of the claims, the finality of the Office Action dated January 11, 2005, is improper. Withdrawal of the finality of the Office Action dated January 11, 2005, is respectfully requested.

I. Rejection of Claims 28, 35, 41, and 47 Under 35 U.S.C. §103(a)

Claims 28, 35, 41, and 47 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,658,568 to Ginter, et al. ("Ginter") in view of U.S. Patent No. 6,816,900 to Vogel, et al. ("Vogel"), and further in view of U.S. Patent No. 6,233,341 to Riggins ("Riggins"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claims 28, 35, 41, and 47 recite automatically obtaining a second certificate for a user comprising accessing a registration server using a user's server and a first certificate of the user to create a connection that authenticates both a user's server identity via a server certificate of the

user server and a user's identity via the user's first certificate. Ginter teaches a method for secure, automated transaction processing for use in electronic commerce and electronic rights and transaction management over an electronic network (Abstract). Ginter, however, does not teach or suggest authenticating both a user's server identity via a server certificate of the user server and the user's identity via the user's first certificate. Ginter also does not teach or suggest sending the public key from the authority to another authority to be signed.

Vogel teaches maintaining and updating root certificates on a computer (Abstract). The Office Action dated January 11, 2005, asserts that Vogel discloses "authenticating based on multiple certificates" (page 3) and thus teaches authentication of both a user's server identity via a server certificate of a user server and a user's identity via the user's first certificate, as recited in claims 28, 35, 41, and 47. It is respectfully submitted that this assertion of how the teachings of Vogel are applied in the rejection of claims 28, 35, 41, and 47 is improper. Specifically, "authenticating based on multiple certificates" is an overgeneralization of "authentication of both a user's server identity via a server certificate of a user server and a user's identity via the user's first certificate", as recited in claims 28, 35, 41, and 47. Vogel teaches that, to establish a secure connection between a client computer and a server computer, the server computer transmits a server certificate to the client computer (col. 4, ll. 10-13). The client computer uses the server certificate to verify that the server computer can be trusted (col. 4, ll. 13-15). Thus, Vogel teaches that the server certificate is a certificate corresponding to the server to which a user (client) wishes to obtain access. The server computer, as taught by Vogel, sends the server certificate to a user for the user's computer to authenticate it. Therefore, Vogel does not teach or suggest authenticating a user's server identity via a server certificate of a user server to access a registration server.

The Office Action dated January 11, 2005, further asserts that "[i]t would have been obvious to one of ordinary skill in the art at the time the invention was made to authenticate based on multiple certificates and establish a secure connection therefrom, since Vogel states, at column 4, lines 31-37, that such a modification deny [sic] access to users that could not verify the server identity thereby keeping malicious users from obtaining a second certificate." (page

3). It is respectfully submitted that this is a misstatement of Vogel. The cited section of Vogel states:

> "If such a certificate chain can be established by client computer, then the server computer which transmitted the server certificate is verified as being trusted and a secure connection can be established. However, if such a certificate chain cannot be established, then the server computer is not trusted and a secure connection to the server computer cannot be established." (col. 4, ll. 31-37).

Vogel teaches only the establishment of a secure connection, and is completely silent on the obtainment of a second certificate. Therefore, automatically obtaining a second certificate for a user using a first certificate and a server certificate, as recited in claims 28, 35, 41, and 47, is neither taught nor suggested by Vogel.

The addition of Riggins does not cure the above mentioned deficiencies of Ginter and Vogel to teach automatically obtaining a second certificate for a user comprising accessing a registration server using a user's server and a first certificate of the user to create a connection that authenticates both a user's server identity via a server certificate of the user server and a user's identity via the user's first certificate, as recited in claims 28, 35, 41, and 47. In addition, Riggins teaches that a certifying authority verifies the identity and other information about a user, creates a signed certificate, and sends the signed certificate to the user (col. 1, ll. 40-67). Additionally, Riggins teaches only that the certifying authority signs the public key (col. 1, ll. 59-67). However, Riggins does not teach or suggest sending the public key from the authority to another authority to be signed, as recited in claims 28 and 41. Therefore, Ginter, Riggins, and Vogel, individually or in combination, do not teach or suggest the elements of claims 28, 35, 41, and 47. Withdrawal of the rejection of claims 28, 35, 41, and 47, as well as claims 29-34, 36-40, 42-46, and 48-52 which depend therefrom, respectively, is respectfully requested.

II. Rejection of Claim 29 Under 35 U.S.C. §103(a)

Claim 29 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Ginter in view of Vogel in view of Riggins as applied above, in further view of U.S. Patent No. 6,108,788

to Moses, et al. ("Moses"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claim 29 recites sending a backup copy of the private key from the authority to a key recovery authority. Moses teaches a certificate management system and method that allows a requester to customize certificates (Abstract). The addition of Moses to Ginter, Vogel, and Riggins does not cure the deficiencies of the Ginter, Vogel, and Riggins to teach or suggest claim 28, from which claim 29 depends. Accordingly, for at least the reasons described above with regard to claim 28, claim 29 should be patentable as well. Withdrawal of the rejection of claim 29 is respectfully requested.

III. Rejection of Claims 30-34, 36-40, 42-46, and 48-52 Under 35 U.S.C. §103(a)

Claims 30-34, 36-40, 42-46 and 48-52 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Ginter in view of Vogel in view of Riggins as applied above, in further view of Haber, et al. ("Haber") (U.S. Patent No. 5,373,561). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claims 30-34 depend from claim 28, claims 36-40 depend from claim 35, claims 42-46 depend from claim 41, and claims 48-52 depend from claim 47. However, Haber does not cure the aforementioned deficiencies of Ginter in view of Riggins. In particular, Haber does not teach or suggest automatically obtaining a second certificate for a user using a first certificate comprising the authentication of both a user's server identity via a server certificate of a user server and a user's identity via the user's first certificate to access a registration server, as recited in claims 28, 35, 41, and 47, from which claims 30-34, 36-40, 42-46, and 48-52 depend, respectively. Therefore, claims 30-34, 36-40, 42-46, and 48-52 should also be allowed over the cited art. Withdrawal of this rejection is respectfully requested.

CONCLUSION

In view of the foregoing remarks, Applicant respectfully submits that the present application is in condition for allowance. Applicant respectfully requests reconsideration of this application and that the application be passed to issue.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Respectfully submitted,

Date 3/8/05

Christopher P. Harris
Registration No. 43,660

CUSTOMER NO.: 26,294

TAROLLI, SUNDHEIM, COVELL, & TUMMINO L.L.P.
526 SUPERIOR AVENUE, SUITE 1111
CLEVELAND, OHIO 44114-1400
Phone: (216) 621-2234
Fax: (216) 621-4072